Stewart R. Pollock (SBN 301356)
spollock@edelson.com
EDELSON PC
123 Townsend Street,
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Putative Class

Additional Counsel on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

LATISHA SATCHELL, individually and on behalf of all others similarly situated,

Plaintiff,

v.

SONIC NOTIFY, INC. d/b/a SIGNAL360, a Delaware Corporation, YINZCAM, INC., a Pennsylvania Corporation, and GOLDEN STATE WARRIORS, LLC, a California Limited Liability Company,

Defendants.

Case No. 4:16-CV-04961-JSW

PLAINTIFF'S COMBINED RESPONSE IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS

Date: January 27, 2017
Time: 9:00 a.m.
Room: Courtroom 5, 2nd Floor
1301 Clay Street
Oakland, California 94612

Judge: Hon. Jeffrey S. White

TABLE OF CONTENTS

TABLE OF AUTHORITIES

United States Supreme Court Cases:

United States Circuit Court of Appeals Cases:

United States District Court Cases:

State Court Cases:

Statutory Provisions:

Rules:

Other Authorities:

SUMMARY OF ARGUMENT

Defendants' motions to dismiss Plaintiff LaTisha Satchell's two-count complaint for violation of the Electronic Communications Privacy Act (the "Wiretap Act"), 18 U.S.C. § 2510, should be denied. Defendants first argue that Ms. Satchell lacks Article III standing under *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), because she has only alleged a "technical" statutory violation of the Act. Here, however, both history and the judgment of Congress establish that the intangible harms Ms. Satchell suffered constitute a concrete injury sufficient to confer standing as articulated by the Supreme Court in *Spokeo*. Historically, courts have entertained suits for invasion of privacy, and modern-day courts have reasoned that claims brought under the Wiretap Act are closely related to these common-law torts. *See Matera v. Google Inc.*, No. 15-cv-04062, 2016 WL 5339806, at *9 (N.D. Cal. Sept. 23, 2016); *Romero v. Securus Techs., Inc.*, No. 16-cv-1283, 2016 WL 6157953, at *5 (S.D. Cal. Oct. 24, 2016). Moreover, in enacting the Wiretap Act, Congress created a substantive right to privacy in one's communications. *Matera*, 2016 WL 5339806, at *16; Pub. L. No. 90-351, § 801(b), (d) (1968). Taken together, Ms. Satchell has suffered a concrete injury, and one independent of her additional, well-pleaded allegations of "wear and tear" on her smartphone.

Defendants contend that Ms. Satchell's oral communications were never "intercepted" or "used." *See* 18 U.S.C. § 2511(1)(a), (d). "Aural acquisition"—and thus, interception—can occur "through the use of any electronic, mechanical, or other device," including a mobile app. 18 U.S.C. § 2510(4). Contrary to Defendants' argument, acquisition is not contingent upon transmission, hearing, or latter possession. *See United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976). Because Ms. Satchell clearly states that for months, Defendants—through the App—captured everything she said as the App ran on her smartphone, and then used her audio data in attempts to deliver marketing messages, (*see* Compl. ¶¶ 3–5, 31, 34, 36, 50, 59), she has stated a claim for interception, which is all that is necessary to pursue a private right of action under the Wiretap Act. *See* 18 U.S.C. § 2520. Further, because all three Defendants worked together to build and bring the App to consumers (as opposed to providing a mere "avenue" for Signal360's audio beacon technology to function), they are each liable for the unlawful interceptions at issue here.

Both motions to dismiss should accordingly be denied.

INTRODUCTION

When Plaintiff LaTisha Satchell downloaded the Golden State Warriors mobile application (the "App") onto her smartphone to track her favorite basketball team, she never imagined that *she* would be the one being monitored. And yet, that is precisely what Defendants Golden State Warriors ("Golden State" or "GSW"), Sonic Notify, Inc. d/b/a/ Signal360 ("Signal360"), and YinzCam, Inc. ("Yinzcam") engineered their popular App to do. Through their implementation of Signal360's "audio beacon" technology, Defendants employed App users' smartphone microphones to continually capture and process *all* background audio, including conversations. Defendants then use the App to filter the recorded audio and identify unique signals, or "beacons," which then trigger the delivery of custom-tailored content, promotions, and advertisements directly to users' smartphones. Because Defendants never sought users' consent for this constant and surreptitious recording activity, Ms. Satchell filed a two-count class action complaint for violation of the Electronic Communications Privacy Act (the "Wiretap Act"), 18 U.S.C. § 2510, *et seq.*

Through two separate motions, all three Defendants now move to dismiss pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). First, and relying on *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), Defendants claim that Ms. Satchell lacks Article III standing because their recording activity has not resulted in a "concrete" injury. But this argument completely misapplies *Spokeo*: not only does Ms. Satchell allege a *substantive* (rather than merely procedural) violation of the Wiretap Act, Defendants also ignore that the Wiretap Act guards against intangible harms that are firmly rooted in common-law privacy torts and protects substantive privacy interests that Congress explicitly sought to protect in enacting the Wiretap Act. Put simply, history and judgment of Congress establish that the invasion of privacy Ms. Satchell suffered is a concrete injury sufficient to confer Article III standing. Second, Defendants claim that they never "intercepted" or "used" Ms. Satchell's oral communications to their advantage, primarily because their App never transmitted the captured audio from Ms. Satchell's smartphone to Defendants' remote servers, and cannot face liability. But Defendants' argument misses the point and runs contrary to the vast majority of case law—including binding Ninth Circuit precedent—confirming that the very act of *capturing* oral communications (whether through a telephone bug or through software installed on a

smartphone) is an unlawful acquisition within the meaning of the Wiretap Act; it doesn't matter whether Defendants did anything nefarious with the captured communications. For all these reasons, explained fully herein, Defendants' motions should be denied in their entirety.

FACTUAL BACKGROUND[1]

Defendant Golden State, Signal360, and YinzCam worked together to bring basketball fans a mobile application—the App—that lets fans keep up with the Golden State Warriors NBA team and, at the same time, lets Defendants deliver individually tailored content, promotions, and advertisements triggered by a consumer's (or, more specifically, a consumer's smartphone's) physical location. (Compl. ¶¶ 2, 3.) While this project is on the forefront of user-specific interactivity—and, from Defendants' perspective, monetization—its undisclosed functionality requires that users' smartphones *constantly* record and monitor all background audio, which necessarily includes *all* of its users' conversations. (*Id.* ¶¶ 23, 32.) And while there may be a hypothetical consumer who is glad to let *three* separate entities capture and analyze all of his or her daily interactions—e.g., from ordering lunch, to conversing with colleagues at the workplace, to private conversations at the family dinner table—Defendants never told any of their users about the App's invasive recording and audio usage practices. (*Id.* ¶¶ 6, 28.)

Acting alone, none of the Defendants here could have independently brought consumers a product featuring portable audio beacon technology (that was Signal360), integrated into a smartphone application (that was YinzCam), and delivered to an existent and eager user base (that was Golden State). (*Id.* ¶¶ 2, 3.) Together, however, Defendants were able to co-opt thousands of consumers who already downloaded the App and convince thousands of additional consumers to

---

[1] Without making a request for judicial notice, Defendants' briefing includes several references to materials or facts far outside the four corners of the Complaint. For example, the GSW Memorandum quotes from—at length—the *current* version of the Signal360 privacy policy to, presumably, suggest that aspects of the App's recording practices were disclosed. (GSW Mem. at 5 n. 5.) Not only is the current version of this document not referenced in the Complaint, discovery will confirm that Defendants made *no* efforts to direct any of its App users to the listed URL (and, thus, it will not have any relevance to this case moving forward). In any event, this reference—and the others like it (*see, e.g.*, GSW Mem. at 5 n. 6, n. 7)—may not be considered on Defendants' motions. *See Ismart Int'l Ltd. v. I-Docsecure, LLC*, No. 04-cv-3114, 2005 WL 588607, at *6 (N.D. Cal. Feb. 14, 2005) (citing *Van Buskirk v. Cable News Network, Inc.*, 284 F.3d 977, 980 (9th Cir. 2002) ("[A] court may look only at the face of the complaint and documents attached to or referenced in the complaint to decide a motion to dismiss.")).

install a constant listening device on their smartphone (without, of course, explaining that the App also functioned as a traditional "bug") and, as a result, deliver those consumers highly targeted advertisements. (*Id.* ¶ 14.)

As alleged, the Signal360 audio beacon technology that the App employs, which was coded into the App by YinzCam, detects and responds to unique audio signals generated by specialized speakers scattered throughout various locations. (*Id.* ¶ 22.) For the App to "hear" and respond to these unique audio signals, it must be allowed constant access to the microphone on the smartphone on which it runs and must record all background audio at all times. (*Id.* ¶¶ 23, 32.) Accordingly, the App was programmed to activate each user's microphone as soon as the App is opened, and to constantly monitor the microphone's audio input for Signal360's beacons—i.e., as an individual user moves from place to place, engages in conversations, etc.—recording and then analyzing all background audio in the process. (*Id.* ¶¶ 31, 32.) Once the App user comes within range of a Signal360 speaker and an audio beacon is recorded by a user's smartphone (i.e., in addition to all the other audio sounds around the user), the App will analyze that recording, detect the beacon, and then trigger the delivery of location-based marketing messages to the user. (*See id.* ¶¶ 3, 22, 23, 50, 59.)

To assure constant surveillance, the App must continuously capture a smartphone's audio input, even if a user isn't actively using the App itself. Thus, the App will continue recording and analyzing all of the microphone's audio input until the App is completely closed—that is, when the consumer shuts off his/her smartphone or "hard closes" the App (e.g., by manually stopping the Signal360 process). (*Id.* ¶ 30.) That is to say, the App, by design, "listens" to and records a microphone's audio input even when the consumer is not actively using the App, but merely has the App running in the background of his or her smartphone. (*Id.*) The App does not seek users' permission to access their microphones for this purpose. (*Id.* ¶ 30.) Nor does the App request that users "opt-in" to Signal360's beacon technology. (*Id.* ¶ 27.)[1]

[1] Golden State and Signal360 suggest (without any explanation) that Ms. Satchell alleges "an 'interception' in a conclusory fashion." (GSW Mem. at 8 n. 10.) Given the detailed and technical allegations found throughout the Complaint—which explain how Defendants designed, developed, distributed, and maintained the App, which constantly records audio, (*see, e.g.*, Compl. ¶¶ 22, 30-32)—Defendants' argument shouldn't be taken seriously.

Ms. Satchell opened the App immediately after downloading it in April of 2016. (*Id.* ¶ 33.) For the next four months, until about July 11, 2016, she used the App to follow the progress of the Golden State Warriors and, thinking nothing of it, allowed it to run in the background on her smartphone. (*Id.*) Because Defendants did not explicitly seek Ms. Satchell's permission to record and analyze all detectable audio, she had no idea that her private conversations were being surreptitiously recorded and analyzed. (*Id.* ¶ 35.) During this timeframe, Ms. Satchell carried her smartphone on her person. (*Id.* ¶ 34.) The App—running continuously in the background—used her smartphone's microphone to record and contemporaneously analyze all background audio as Ms. Satchell traveled to various locations where she expected her conservations to remain private. (*Id.* ¶ 35.)

ARGUMENT

I. Ms. Satchell Has Article III Standing.

"A party seeking to invoke the federal court's jurisdiction bears the burden of demonstrating that [she] has standing to sue." *Supply Pro Sorbents, LLC v. Ringcentral, Inc.*, No. 16-cv-02113, 2016 WL 5870111, at *2 (N.D. Cal. Oct. 7, 2016). Standing has three components: (1) a concrete and particularized injury that is (2) traceable to the defendants' conduct and (3) redressable by a favorable judicial decision. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). Here, Defendants contend only that Ms. Satchell has not suffered a "concrete" injury and, relying on the Supreme Court's decision in *Spokeo*, say that Ms. Satchell lacks standing because she asserts a "mere technical violation" of the Wiretap Act. (*See* GSW Mem. at 11–12; YinzCam Mem. at 5–8.) But this attack ignores that Ms. Satchell's entire Complaint is based on a violation of the Act's core *substantive* protection (i.e., an unauthorized recording of private conversations using a device) and, in line with *Spokeo*, readily alleges a concrete Article III injury.

In *Spokeo*, the Court reiterated that "Article III standing requires a concrete injury even in the context of a statutory violation." 136 S. Ct. at 1549. This has long been the law. *See Raines v. Byrd*, 521 U.S. 811, 819-20 & n.3 (1997). But as *Spokeo* further emphasized, in some cases "a plaintiff…need not allege any *additional* harm beyond the one Congress has identified." 136 S. Ct. at 1549 (emphasis in original). In other words, "*Spokeo* clearly rejects [Defendants'] position that a

plaintiff may *never* rely solely on the purported statutory violations alone as the basis for Article III standing." *Matera v. Google Inc.*, 2016 WL 5339806, at *9 (N.D. Cal. Sept. 23, 2016) (quotations omitted) (emphasis in original). Indeed, *Spokeo* explains that while "bare procedural [statutory] violation[s]" *may* be insufficient to confer Article III standing, "intangible injuries can nevertheless be concrete." *Spokeo*, 136 S. Ct at 1549.

"In determining whether an intangible harm [deriving from a statutory violation] constitutes injury-in-fact, both history and the judgment of Congress play important roles." *Id.*; *see Matera*, 2016 WL 5339806, at *9 ("When evaluating whether the violation of a statute establishes concrete injury, *Spokeo* instructs courts to consider [these] two factors."). Here, Ms. Satchell's allegations regarding Defendants' violation of the Wiretap Act suffice to establish her standing to sue, even absent consequential harm.[2] Far from asserting a "technical" violation of the Wiretap Act, Ms. Satchell alleges that Defendants' violation of the Wiretap Act invaded her privacy in a cognizable way. Unauthorized surveillance by private parties, whether it be eavesdropping or tapping a phone—snooping, essentially—has long been actionable in the courts, both in England and in America. And it is the snooping itself, not anything done with the information (blackmail, monetization, etc.), that has traditionally given rise to an injury recognized at common law. That history carried forward into the Wiretap Act, which originally was drafted to prohibit both police and private parties from bugging phones without judicial approval—a prohibition that has expanded to include unauthorized monitoring of *all* electronic communication, whether or not those

[2] Ms. Satchell *also* alleges harm flowing from Defendants' conduct. (Compl. ¶¶ 52, 61.) Defendants say that those allegations—i.e., regarding the "wear and tear" to her phone—are too *de minimis* to constitute cognizable harms and also are unconnected to Defendants' statutory violations—and, thus, cannot count as a concrete Article III injury. (GSW Mem. at 12–15; YinzCam Mem. at 6–8.) Neither argument is availing. As to the latter, Ms. Satchell's phone loses battery life much faster than it otherwise would *because* the App turns the built-in microphone on, (*see* Compl. ¶¶ 5, 30), so these allegations present no problem with respect to traceability. Further, contrary to Defendants' representations, many courts—including in this District—have acknowledged that wear and tear does constitute cognizable harm sufficient to convey Article III standing. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1054 (N.D. Cal. 2012); *Goodman v. HTC Am., Inc.*, No. 11-cv-1793, 2012 WL 2412070, at *7 (W.D. Wash. June 26, 2012). (*See also* GSW Mem. at 15, n.15 (acknowledging similar cases); YinzCam Mem. at 7 n.2 (same).) In any event, while these allegations provide an *additional* basis for Ms. Satchell's standing to sue (i.e., beyond Defendants' violation of the substantive protections provided by the Wiretap Act), the Court need not reach these issues for the reasons discussed in Section I.

communications were subsequently read, parsed, analyzed, or disseminated. *See* 18 U.S.C. §§ 2510(4), 2511(1)(a).

In other words, just as at common law, the interests protected by the Wiretap Act are invaded when, as here, a defendant intercepts a plaintiff's communications without authorization. Thus, a violation of the Wiretap Act's central prohibition, and an invasion of the primary privacy interests protected by the Act, is anything but a "technical" statutory violation. Contrary to Defendants' overwrought assertion, Ms. Satchell does not allege "an entirely novel form of intangible injury," but instead alleges a centuries-old intangible harm that was given new life by Congress's enactment of the Wiretap Act. Under *Spokeo*, Ms. Satchell has suffered a concrete injury, and she has standing to sue.

A. Ms. Satchell's injury is closely related to an injury recognized at common law.

Spokeo teaches that "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." 136 S. Ct. at 1549. A harm closely related to one recognized by the common law will be concrete under *Spokeo*. Here, the intangible harms that derive from a violation of the Wiretap Act (i.e., an intentional interception of any wire, oral, or electronic communication), 18 U.S.C. § 2511(1)(a), meet that test because the Act protects against the same types of harms that permitted a plaintiff to sue for invasion of privacy in English or American courts.

In England, common-law judges recognized that "eavesdroppers, or such as listen under walls or windows, or the eaves of a house,…are a common nuisance" and could be haled into manorial courts. 4 Blackstone, Commentaries on the Laws of England 169 (1769). Early American courts likewise recognized that "eaves-dropping is an indictable common law offense." *State v. Pennington*, 40 Tenn. 299, 301 (Tenn. 1859) (citing *State v. Williams*, 2 Tenn. 108 (Tenn. 1808)). Moreover, American common-law courts have regularly entertained suits for invasions of privacy more broadly. *See, e.g., Romero v. Securus Techs., Inc.*, 2016 WL 6157953, at *5 (S.D. Cal. Oct. 24, 2016) (denying motion to dismiss state-law wiretap claim based on common-law history of suits for invasion of privacy); *Yershov v. Gannett Satellite Info. Network, Inc.*, No. 14-cv-13112, 2016 WL 4607868, at *8 (D. Mass. Sept. 2, 2016) (denying motion to dismiss statutory privacy claim

because "an individual's right to privacy…has long been regarded as providing a basis for a lawsuit in English or American courts") (quotation omitted); *Thomas v. FTS USA, LLC*, No. 13-cv-825, 2016 WL 3653878, at *10 (E.D. Va. June 30, 2016) (denying motion to dismiss Fair Credit Reporting Act claim based on standing challenge, noting that "common law has long recognized a right to personal privacy"). *Matera*, which dealt with a claim under the Wiretap Act for unauthorized scanning of the plaintiff's emails, is of particular relevance here. In that case, Judge Koh concluded that the Wiretap Act and an analogous California state law were "similar to common law invasion of privacy in both their substantive prohibitions and their purpose." *Matera*, 2016 WL 5339806, at *10. Denying the defendant's motion to dismiss, Judge Koh specifically noted that in light of this common-law tradition, the "unauthorized interception of communications may give rise to a legally cognizable injury." *Id.* at *11.

Ms. Satchell's Wiretap Act claim alleges a classic invasion of privacy. *See id.* She alleges that the App works much like a "bug": it turns the phone's microphone on, captures, and then analyzes all audio within the microphone's range. (*See* Compl. ¶¶ 4–5, 23, 30–31.) This kind of surreptitious listening device is the archetypal target of an intrusion-upon-seclusion claim. The Restatement explains that one type of intrusion occurs through "the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by…tapping his telephone wires." Restatement (Second) of Torts § 652B cmt. b. American courts have long heard claims related to the use of technology to intrude upon private conversations, particularly through the telephone. *See, e.g.*, *Hamberger v. Eastman*, 206 A.2d 239, 241-42 (N.H. 1964); *Rhodes v. Graham*, 37 S.W.2d 46, 47 (Ky. 1931).

Moreover, to the extent Defendants believe their extra-record assertions about the nature of their intrusive conduct (e.g., that all audio captured through the App is deleted and that Defendants don't use the majority of the captured audio for any purpose) are well taken,[3] the common law

[3] Defendants, for example, assert that the audio recordings the App makes are "deleted from the phone's buffer memory almost immediately after they are captured," and that the App specifically scans for high-frequency signals emitted by the audio beacons, "discard[ing] the audio data of all other frequencies." (GSW Mem. at 5 n.6, n.7.) These assertions, on top of the fact that they lack relevance to the "interception" issue because they speak to conduct post-capture, are far beyond the pleadings and cannot be considered here.

shows that they are irrelevant to the standing inquiry: "The tort is completed with the *obtaining* of the information by improperly intrusive means." *Pearson v. Dodd*, 410 F.2d 701, 704 (D.C. Cir. 1969) (emphasis added). "The intrusion itself makes the defendant subject to liability." Restatement (Second) of Torts § 652B cmt. b. In fact, in *Hamberger*, the court explicitly rejected the argument that the plaintiffs had failed to state a claim because "there are no allegations that anyone listened or overheard any sounds or voices" picked up by the intrusive "bug." 206 A.2d at 242. Those types of allegations, the court held, were unnecessary. *Id.*; *see also Amati v. City of Woodstock*, 829 F. Supp. 998, 1009-11 (N.D. Ill. 1993) (rejecting similar argument).

To be sure, some jurisdictions conclude that the common-law tort is incomplete if the recorded conversations are not listened to. *See Oliver v. Pac. Nw. Bell Tel. Co.*, 832 P.2d 1295, 1299 (Or. Ct. App. 1981); *Marks v. Bell Tel. Co. of Pa.*, 331 A.2d 424, 431 (Pa. 1975). But undoubtedly, this rule "represent[s] the minority view." *Koeppel v. Speirs*, 808 N.W.2d 177, 184 (Iowa 2011) (rejecting narrower rule). And regardless, all that Article III requires is a "close relationship" to a common-law harm. *See Spokeo*, 136 S. Ct. at 1549. Thus, even if the intrusion tort in some jurisdictions is narrower than the Wiretap Act, there is still a close relationship between the harms guarded against by the Wiretap Act and by the common law. *See Matera*, 2016 WL 5339806, at *11 ("That the Wiretap Act [is] not identical in every respect to invasion of privacy does not preclude violations of the Wiretap Act…from constituting injury in fact."); *see also Spokeo*, 136 S. Ct. at 1549 (holding that Congress is empowered to "elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law") (quotations omitted). By capturing Ms. Satchell's and the putative class' communications, Defendants caused them to suffer concrete injury consistent with *Spokeo*.

B. Congress's judgment also demonstrates that Ms. Satchell's injury is concrete.

Spokeo instructs Courts to heed Congress's judgment in determining whether an intangible harm is concrete. *See* 136 S. Ct. at 1549. In assessing this fact, "many courts since *Spokeo* have placed dispositive weight on whether a plaintiff alleges the violation of a substantive, rather than procedural, statutory right…[C]ourts have generally found…that a plaintiff alleging violation of a substantive statutory right has Article III standing." *Matera*, 2016 WL 5339806, at *12.

As *Matera* recognizes, "the Wiretap Act…create[s] substantive rights to privacy in one's communications." *Id.* at 13. The Act "is designed to prohibit 'all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officials.'" *Greenfield v. Kootenai County*, 752 F.2d 1287, 1388 (9th Cir. 1985) (quoting S. Rep. No. 90-1097); *see also DirecTV, Inc. v. Webb*, 545 F.3d 837, 850 (9th Cir. 2008) ("The Wiretap Act is aimed largely at privacy protection."). Congress specifically noted that it first created wiretapping prohibitions "in order to protect effectively the privacy of wire and oral communications" and "to safeguard the privacy of innocent persons." Pub. L. No. 90-351, § 801(b), (d) (1968).

The statutory violations alleged by Ms. Satchell invoke the core protections Congress gave to these privacy interests. Ms. Satchell alleges that the App effectively hijacks her phone's microphone, capturing and analyzing all of her private conversations. These acts, like those at issue in *Matera*, plainly infringe on a substantive statutory right, *see Matera*, 2016 WL 5339806, at *13 (holding that "the Wiretap Act…create[s] substantive rights to privacy in one's communications," and, thus, an "unlawful intercept[ion]" in violation of the Act is not a "bare procedural violation."), for which Congress has authorized suit without a showing of actual harm. *See id*. (noting that, under the Wiretap Act, a "plaintiff may recover *either* actual damages, statutory damages, or injunctive relief."). Indeed, this recognized distinction between substantive and procedural rights demonstrates why Defendants' reliance on *Nei Contracting & Engineering, Inc. v. Hanson Aggregates Pac. Sw., Inc.*, No. 12-cv-01685, 2016 WL 4886933, at *5 (S.D. Cal. Sept. 15, 2015), is misplaced. (*See* GSW Mem. at 12.) Although that case dealt with a "wiretap claim," the injury in that case derived from the defendant's failure to provide statutorily mandated notice. *Id*. Because *Nei Contracting* involved a procedural violation of the Act—rather than the substantive one alleged here—it is inapposite. *See Spokeo*, 136 S. Ct. at 1550.

This common-law history and judgment of Congress therefore establishes that Ms. Satchell has suffered a concrete injury and, thus, has standing to sue.

II. Ms. Satchell Has Stated a Claim Under the Wiretap Act.

Turning to the substantive allegations of the Complaint, Ms. Satchell states a claim under the Wiretap Act because she has plausibly alleged that the Defendants "intercepted" her oral

communications as soon as the App began recording, and then "used" her oral communications in attempts to deliver targeted marketing messages.

A complaint survives a Rule 12(b)(6) motion to dismiss when it contains "enough facts to state a claim for relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Detailed factual allegations are not required, and "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). In evaluating a defendant's Rule 12(b)(6) motion, a court construes the complaint in the light most favorable to the plaintiff, accepting all well-pleaded facts as true, and drawing all reasonable inferences in the plaintiff's favor. *See Dahlia v. Rodriguez*, 735 F.3d 1060, 1066 (9th Cir. 2013). Under this liberal standard, both motions should be denied in their entirety.

The Wiretap Act makes it unlawful to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," and to "intentionally use[], or endeavor[] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." 18 U.S.C. § 2511(1)(a), (d).[4] Because Ms. Satchell has plausibly alleged that Defendants intercepted her communications through the App, which they together built and brought to consumers, and then used those communications to deliver marketing messages, she has stated a claim under the Wiretap Act.

A. Ms. Satchell alleges that Defendants intercepted her oral communications.

To start, Defendants challenge whether Ms. Satchell has alleged an "interception" of her oral communications. But under the Wiretap Act—and consistent with the Ninth Circuit's interpretation of it—Defendants' unlawful "interceptions" began as soon as the App was opened and the microphone began listening and recording, continuously doing so (seemingly over a four-month

[4] While there is no liability under the Wiretap Act where one party to the communication consents to an interception, *see* 18 U.S.C. § 2511(2)(d), Defendants do not attempt to argue that the consent exemption applies here.

period) without consent. These facts readily state an actionable interception.

The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The Ninth Circuit, among others, has held that "the most reasonable interpretation of the statutory definition of interception is that an interception occurs" both at the *site* of the actual interception (such as "where [a] tapped phone is located") *and* where the intercepted communications are "overheard" or reviewed by a third party. *United States v. Luong*, 471 F.3d 1107, 1109 (9th Cir. 2006). In so holding, the Ninth Circuit agreed that "[i]t seems clear that when the contents of a wire communication are *captured*…in any way, an interception occurs at that time. Such an interception plainly occurs at…the situs of the [device] itself…" *Id.* (quoting *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992) (emphasis added). Consistent with this definition, the acquisition—and thus, the interception—of an oral communication occurs first where and when a device makes an unauthorized recording. *See United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976) ("If a person secrets a recorder in a room and thereby records a conversation between two others, an 'acquisition' occurs at the time the recording is made."), *disagreed with on other grounds Noel v. Hall*, 568 F.3d 743, 749 n.9 (9th Cir. 2009); *Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) (holding that defendant who recorded tapes but did not listen to them was "not insulate[d] from liability for the invasion of privacy it helped to occasion"); *Amati*, 829 F. Supp. at 1008 ("Whether the communication is heard by the human ear is irrelevant."); *see also United States v. Nelson*, 837 F.2d 1519, 1527 (11th Cir. 1988) ("[T]he term 'intercept' as it relates to 'aural acquisitions' refers to the place where a communication is initially obtained regardless of where the communication is ultimately heard.").

Here, Ms. Satchell plausibly alleges an actionable interception occurred as soon as Defendants, through the App, began recording her conversations. (*See* Compl. ¶¶ 48, 57.).[5] As the

[5] The fact Golden State and Signal360 contend that each recording is short and is overwritten by the next one is irrelevant, as nothing in the statute requires a communication to be permanently recorded before it is "intercepted." *In re Innovatio IP Ventures, LLC Patent Litig.*, 886 F. Supp. 2d 888, 892 (N.D. Ill. 2012) (noting that "record[ing] in a permanent medium…is nowhere found in the Wiretap Act…[and that] an individual's [communication] activity can be chilled merely by the knowledge that a third party has the power to acquire, however briefly, the contents of his communications."). Moreover, as noted above, Defendants' extraneous allegations go beyond the

Fifth Circuit asked, "In a forest devoid of living listeners, a tree falls. Is there a sound? The answer is yes, if an active tape recorder is present, and the sound might be thought of as 'aurally acquired' at (almost) the instant the action causing it occurred." *Turk*, 526 F.2d at 657–58 n. 2. Stated plainly, once a communication is acquired through the use of "any electronic, mechanical, or other device," an interception has occurred. 18 U.S.C. § 2510(4). The Act does not require a subsequent transmission, hearing, or possession. *See In re State Police Litig.*, 888 F. Supp. 1235, 1264 (D. Conn. 1995) (noting that device requirement "suggests that it is the act of diverting, and not the act of listening, that constitutes an 'interception.'"). Indeed, "even if [an] individual was assured *no one* would listen to his conversations," recording alone chills speech "because the individual's privacy interests are no longer autonomous." *Amati*, 829 F. Supp. at 1008; *accord In re Innovatio*, 886 F.Supp 2d 892. *See also Jacobson*, 592 F.2d at 522 ("In enacting Title III Congress intended to establish sanctions that would deter illegal invasions of privacy through wiretapping…we do not believe that Congress meant to allow those tapping phones to determine the possible scope of civil liability by their limiting who among them would listen to the tapes."). Here, because Ms. Satchell has alleged that Defendants captured portions of her oral communications using the App, (*see* Compl. 5, 31, 50, 59),[6] whether those communications were subsequently deleted or listened to by someone else is wholly irrelevant to her claim.

None of Defendants' arguments defeat these straightforward allegations. First, Golden State and Signal360 contend that no acquisition occurred because "the App [n]ever caused any audio data of any kind…to be transmitted beyond Plaintiff's phone." (GSW Mem. at 8.) But as explained at length above, whether a *subsequent* transmission of Ms. Satchell's communications occurred is irrelevant to her claim; all that matters is Defendants *captured* her communications using the App.

Complaint and, thus, are not well taken at this early stage of the litigation. Further discovery is necessary to assess the App's technical specifications and determine what relevance—if any—they have to Ms. Satchell's claims.

[6] Looking forward, the allegations here have already been evaluated by an independent third party expert, who publicly confirmed that the App "absolutely contains code to record audio" and that "[t]he beacon technology provider could easily change this configuration on their server side to enable [or disable] recording in the app." Dan Goodin, *Golden State Warriors Android app constantly listens to nearby audio, fan says [Updated]*, Ars Technica (Sept. 1, 2016), http://arstechnica.com/tech-policy/2016/09/golden-state-warriors-android-app-constantly-listens-to-nearby-audio-fan-says/.

Likewise, Defendants' reliance on *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998) and *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015), for the proposition that "acquisition" refers to "the act of acquiring, or coming into possession of," is similarly misplaced. (GSW Mem. at 7.)[7] While both *Smith* and *Carrier IQ* discuss the "ordinary meaning" of the term "acquisition," neither case holds, or even suggests, that acquisition of an oral communication can only occur after a recording is transmitted to and/or heard by a third party. Rather, both cases hold exactly the opposite and fall in line with the commonsense view discussed above—i.e., that once a communication is *captured* by a defendant's "electronic, mechanical, or other device," it has been acquired and, thus, intercepted.[8] 18 U.S.C. § 2510(4); *see, e.g.*, *In re Carrier IQ, Inc.*, 78 F. Supp. 3d at 1076 (quoting *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (providing definition of "acquisition" cited by Defendants and then explaining that "[the Ninth Circuit] has further held that '[s]uch acquisition occurs 'when the contents of a wire communication are *captured* or redirected *in any way*…'") (emphasis added).

In *Smith*, for example, the Ninth Circuit affirmed the suppression of an unlawfully intercepted wire communication—a hacked voicemail that an individual had forwarded to her own voicemail inbox and subsequently recorded with a handheld recording device. *Smith*, 155 F.3d at 1055. Significantly, the Ninth Circuit found that the "*act of recording the message* with a handheld audiotape-recording 'device' constituted an 'aural or other acquisition'—and, hence, an 'interception'—of the message." *Id.* (emphasis added). In the passage cited by Golden State and Signal360, the Court merely noted that the dictionary definition of the term acquire—"the act of acquiring, or coming into possession of," was "certainly broad enough" to encompass this conduct. *Id.* at 1055. n.7. As such, *Smith* does not establish that acquisition requires a communication to be received or heard by a person in order to be acquired. To the contrary, it was the "act of recording"

---

[7] YinzCam does not cite any case law interpreting the Wiretap Act. Instead, it broadly claims that "Plaintiff has failed to allege any facts demonstrating an 'interception' of an 'oral communication,'" without any explanation of how those terms should be construed. (YinzCam Mem. at 9.) YinzCam's motion to dismiss Ms. Satchell's Wiretap Act claim should be denied for this reason alone.

[8] No Defendant challenges Ms. Satchell's allegation that the App itself is an "electronic, mechanical, or other device" for the purposes of the Wiretap Act. 18 U.S.C. § 2510(4).

the voicemail with a handled recorder that constituted the "aural acquisition" of the communication. *Id.* at 1055. Here, and just like the tape recorder in *Smith*, the App's continual recording activity constitutes an "aural acquisition," and thus, an interception.

Defendants' reliance *In re Carrier IQ* fares no better. That case, like this one, also involved a defendant (Carrier IQ) whose mobile device software intercepted users' communications.[9] *In re Carrier IQ*, 78 F. Supp. 3d at 1059. But unlike this case, the plaintiffs also sued the mobile device manufacturers (e.g., HTC, Samsung, etc.), who, at the behest of telecom carrier customers, installed Carrier IQ's software on their products. *Id.* And while the court acknowledged that the plaintiffs had provided "factual allegations from which it [could] be inferred that the Device Manufacturers were involved in the installation of the Carrier IQ Software on their mobile devices…there [were] no factual allegations that the Device Manufacturers themselves 'seized' or 'redirected' any communications themselves" after installation and, thus, no corresponding liability under the Wiretap Act. *Id.* at 1088.[10] Here, in contrast, Ms. Satchell did not sue the manufacturer of her phone (or Google, who distributed the App in the Play store), because it did not "capture" her communications, even though it did provide an environment that enabled the at-issue interceptions and, in some technical sense, "caused" them. Instead, Ms. Satchell's claims align against Defendants, who "effectuated an interception" by using the App (a "device") to capture users' communications (an "acquisition"). *See In re Carrier IQ, Inc.*, 78 F. Supp. 3d at 1089; 18 U.S.C. § 2510(4). By using the App, it was *Defendants*, and not any other party, who intercepted users'

---

[9] The interceptions at issue in *In re Carrier IQ* involved Carrier IQ's redirection of users' communications to its servers; no part of the opinion, however, suggests that if Carrier IQ had *captured* communications using its software (i.e., as the App does here), it would not have faced liability under the Wiretap Act. Indeed, any such suggestion would run contrary to the Ninth Circuit precedent cited by the *In re Carrier IQ* court itself. *See* 78 F. Supp. 3d at 1076 (acquisition occurs when communications "are captured…in any way") (quoting *Noel v. Hall*, 568 F.3d at 749).

[10] The court also noted that one manufacturer defendant *accidentally* caused certain communications to be stored on the mobile phones and then re-routed to its own remote servers, but "[b]ecause there [were] no factual allegations suggesting that [such] acquisition of communications was intentional, Plaintiffs…failed to plead a basis for Wiretap Act liability…" *In re Carrier IQ, Inc.*, 78 F. Supp. 3d at 1088. Yet, the court in *Carrier IQ* noted that both the software developer (Carrier IQ) and the mobile carriers with which it partnered (e.g., AT&T) "effectuated such an interception" under the Wiretap Act. *Id.* at 1089. Here, Ms. Satchell alleges that *each* Defendant played an active, necessary, and *intentional* role in the at-issue interceptions. (*See* Compl. 2-3, 24.)

background audio, analyzed it, and then delivered targeted advertising to consumers.[11] Thus, just as the "interception" claim was allowed to proceed against the software developer in *Carrier IQ*, but not the device manufacturers, *see id.* at 1082, 1089, here, Ms. Satchell's claim should be allowed to proceed against the three parties who captured (using the App) her oral communications.

Next, Defendants briefly challenge whether Ms. Satchell has plausibly alleged any "oral communications" given that she has not alleged a specific conversation that was recorded. (*See* GSW Mem. at 8; Yinzcam Mem. at 2 n.1.) This argument can be easily dispatched. An "oral communication" is one "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." 18 U.S.C. § 2510(2). Ms. Satchell alleges that for *four months*, the App recorded *everything* she said as it ran on her smartphone, which she carried with her to places "where she would have private conversations."[12] (Compl. ¶ 32.) Because the App's listening activity was continuous from the moment Ms. Satchell first opened the App—and Ms. Satchell never knew it—it is reasonable to assume, particularly at this stage where Ms. Satchell is entitled to all reasonable inferences, that she made communications that she expected would not be subject to interception. *See* 18 U.S.C. § 2510(2).

Finally, Signal360 suggests that it did not unlawfully intercept Ms. Satchell's oral communications because its own speakers emitted high-frequency audio beacon signals and, thus, it was a "party" to any recordings of them. (*See* GSW Mem. at 10 n.12.) This challenge ignores the

---

[11] Golden State and Signal360 also cite *Valentine v. WideOpen W. Fin., LLC*, where the court found that an internet service provider (ISP) had not "acquired" the at-issue communications and, thus, was not liable under the Wiretap Act. 288 F.R.D. 407, 411 (N.D. Ill. 2012). The *Valentine* court's treatment of the ISP is akin to the *In re Carrier IQ* court's treatment of the phone manufacturers: both enabled the interceptions in a technical sense, but were not directly involved in any "acquisition" of communications. Here, Defendants are more like the advertiser defendant in *Valentine*, who contracted with a third-party that "actually accessed the [at-issue] communications when it analyzed them to fashion targeted ads" for the defendant advertiser. *Id.* at 411. The only difference between this case and *Valentine* is that, here, Defendants *captured* communications and then used the App to deliver targeted ads, (Compl. ¶ 31), whereas the *Valentine* defendant *redirected* communications for the same purpose, *Valentine*, 288 F.R.D. at 411. And as discussed herein, *both* capturing and redirecting are "acquisitions" of communications under the Act.

[12] It goes without saying that Ms. Satchell carried her phone everywhere and, thus, had a wide variety of conversations recorded. *C.f. Riley v. California*, 134 S. Ct. 2473, 2484 (2014) (stating that "modern cell phones" "are now a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."). To the extent more specific allegations are required at the pleading stage, Ms. Satchell can readily provide them.

pleadings entirely.[13] Ms. Satchell does not allege that the App only captured "the beacon signals emitted by Signal360's beacons," as Signal360 suggests; she alleges that the App captured *all* background audio, including *all* of her conversations, and only then analyzed and identified the beacon signals from that recorded audio. (Compl. ¶¶ 30-32.) Because Signal360 was not a party to those recorded conversations, its argument fails.

Ms. Satchell has plausibly alleged the interception of her oral communications. The motions to dismiss her Wiretap Act claim should be denied.[14]

B. Ms. Satchell states a claim against all three Defendants.

Golden State and YinzCam attempt to shift the blame for the unlawful interception and use of Ms. Satchell's oral communications onto Signal360, noting that Signal360 developed the audio beacon technology in question. (GSW Mem. at 9; YinzCam Mem. at 10 n.3.) But because Ms. Satchell alleges that all three Defendants played an integral and *necessary* role in developing the App that ultimately intercepted her oral communications, she states a claim against all three Defendants.

The Wiretap Act permits "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" to "recover from the person or entity…which engaged in that violation." 18 U.S.C. § 2520(a). While some courts have interpreted this language as limiting civil liability to those who directly "intercept," "disclose" or "use" communications, *see In re Toys*

---

[13] The scenario proposed by Signal360 would only be possible if the App *only* recorded the high-frequency audio beacon signals. But even if this is hypothetically possible, by using a specially designed microphone that cannot overhear oral communications, for instance, the App was not designed in this manner because it uses smartphone microphones *specifically* designed to pickup oral communications. (Compl. ¶¶ 23, 30, 32.)

[14] Though Defendants Golden State and Signal360 spill much ink on the issue of "use" under 18 U.S.C. § 2511(1)(d), Ms. Satchell need only allege "interception" to invoke the Wiretap Act's civil liability provision, 18 U.S.C. § 2520(a). In any case, Defendants' arguments that the "contents" of Ms. Satchell's oral communications could not have been "used," because the recording length is too short and only high-frequency communications are required miss the mark. (*See* GSW Mem. at 5 n.5; Yinzcam Mem. at 2 n.1.) First, they attempt to read into the Wiretap Act a non-existent exemption based on the *length* of communication taken. Second, they introduce facts not alleged in the Complaint, which only underscores the need for further discovery into the App's technical specifications. Finally, Ms. Satchell's allegations of Defendants using recorded audio to deliver unwanted marketing content align neatly with the purpose of the statute's "use" provision, which is "to reinforce the interception proscription by denying the wrongdoer the fruits of his conduct…and by eliminating the demand for those fruits by third parties." *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 191–92 (5th Cir. 2000) (citation and internal quotations omitted).

R Us, Inc., Privacy Litig., No. 00-cv-2746, 2001 WL 34517252, at *6 (N.D. Cal. Oct. 9, 2001), others have imposed liability on defendants who manufacture, market, sell, and operate the device that is used to do so, *see Luis v. Zang*, 833 F.3d 619, 637 (6th Cir. 2016). Courts have likewise held that a defendant who is "intimately and integrally involved" with facilitating unlawful interception––for instance, by allowing recording software to be implanted on rental computers—may also face direct liability under the Wiretap Act. *See Byrd v. Aaron's, Inc.*, 14 F. Supp. 3d 667, 690 (W.D. Pa. 2014); *Jacobson*, 592 F.2d at 522 (imposing liability on defendant "involved in the setting up of the recording devices").

Here, Ms. Satchell's allegations make clear that each Defendant played an integral and necessary role in bringing the App into existence, and then either endorsed (Golden State) or enabled (YinzCam) the interception and use alleged in the Complaint. With respect to Golden State, Ms. Satchell alleges that Golden State "partnered" with Signal360 specifically to integrate beacon technology into the App so that it could better track and interact with fans, "send them tailored content, promotions, or advertisements based on their locations," and "remain a technological leader among NBA organizations." (Compl. ¶¶ 2–4.) YinzCam, in turn, developed the App into which it intentionally coded Signal360's beacon technology so that Golden State's marketing goals could be fulfilled. (*Id.* ¶ 3.) Defendants thus depended on one another to set up and bring into existence the App that captured (and, thus, intercepted) all of Ms. Satchell's oral communications for a period of four months. Unlike the mobile device manufacturers in *In re Carrier IQ*, who merely provided an "avenue" through which Carrier IQ's software could intercept information and played no further role in the operation of the interception device, *see* 78 F. Supp. 3d at 1089, Golden State and YinzCam did not merely develop a product without regard as to how it would be used.[15] Rather, they both assisted in the continued operation of the interceptions until shortly after this case was filed (i.e., without Golden State and YinzCam, there would be no App and, thus, no interception). (Compl. ¶¶ 2–4.) And unlike the toy retailer in *Toys R Us*, who merely provided the website onto

[15] As noted above, even though the App obviously requires a smartphone to record background audio, Ms. Satchell's phone manufacturer is not named here because it merely provided the "means" that enabled the App's operation and is likely unaware of Defendants' conduct.

which information-tracking "cookies" were planted, *see* 2001 WL 34517252, at *6, Golden State and YinzCam did not simply provide a forum for the alleged interception. Instead, like the software developer and telecom companies in *Carrier IQ*, and along with co-Defendant Signal 360, each Defendant is directly responsible for creating the App that intercepted Ms. Satchell's oral communications (and ultimately used those same communications to deliver marketing materials). Accordingly, Ms. Satchell states a Wiretap Act claim against all three Defendants.

CONCLUSION

For all of these reasons, Defendants' motions to dismiss should be denied in their entirety. In the event this Court grants either motion, however, Ms. Satchell respectfully requests leave to amend her pleadings.

Respectfully submitted,

LATISHA SATCHELL, individually and on behalf of all others similarly situated,

Dated: December 1, 2016

By: /s/ Stewart Pollock
One of Plaintiff's Attorneys

Rafey S. Balabanian*
rbalabanian@edelson.com
Eve-Lynn J. Rapp*
erapp@edelson.com
Stewart R. Pollock (SBN 301356)
spollock@edelson.com
EDELSON PC
123 Townsend Street,
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Putative Class

**Admitted pro hac vice.*